(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11089 A1

(51) International Patent Classification[7]: G07F 19/00, 7/10, G06F 17/60

(21) International Application Number: PCT/SG01/00153

(22) International Filing Date: 20 July 2001 (20.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200004310-9 31 July 2000 (31.07.2000) SG

(71) Applicant *(for all designated States except US)*: **VCHEQ.COM PTE LTD** [SG/SG]; 30 Cecil Street, #11-05/08 Prudential Towers, Singapore 049712 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **WONG, Tien, Poh, Kenneth** [SG/SG]; 30 Cecil Street, #11-05/08 Prudential Towers, Singapore 049712 (SG).

(74) Agent: **O'CONNOR, Teresa**; Raffles City Post Office, P.O. Box 259, Singapore 911709 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

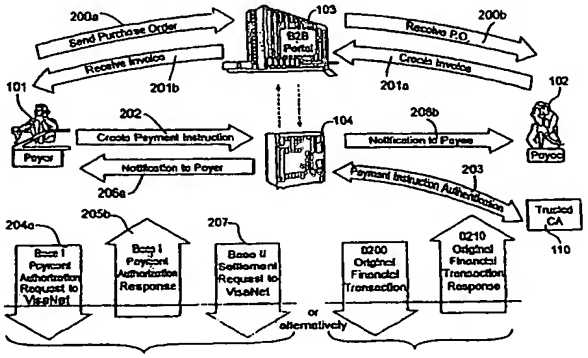
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,*

[Continued on next page]

(54) Title: AN ELECTRONIC FUNDS TRANSFER SYSTEM USING CREDIT CARD SETTLEMENT AND FINANCIAL NETWORK INFRASTRUCTURE



(57) Abstract: An apparatus and method of effecting an electronic transfer of funds between a payer account and a payee account wherein the payer account and the payee account are each held at a financial institution that is a member of a financial settlement network. A payer (10) transmits a purchase order (200) to a payee (102) via a business hub (103), which purchase order identifies the payer. The payee, in response to receipt of the purchase order, transmits an invoice (201) to the payer via the business hub, which invoice identifies the payee account for crediting funds for the purchase. The payer, in response to receipt of the invoice and subsequent to approval of the purchase, transmits a secured payment instruction (202) to a payment gateway (104), which payment instruction identifies the payer account for debiting. The payment gateway, in response to receipt of the secured payment instruction and subsequent to ensuring authenticity (203) of the payment instruction, creates a payment request message (204) for the payer's financial institution (106) and passes the payment request to the settlement network (105). The payment gateway (104), in response to a payment authorisation message (205) from the payer's financial institution, notifies payment approval (206). The financial settlement network (105) facilitates settlement (209) of the transfer on a net basis between the payer's financial institution and the payee's financial institution.

WO 02/11089 A1

SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AN ELECTRONIC FUNDS TRANSFER SYSTEM USING CREDIT CARD SETTLEMENT AND FINANCIAL NETWORK INFRASTRUCTURE

BACKGROUND OF THE INVENTION

(i) Field of the Invention

This invention relates to an electronic payment system that facilitates integration with existing financial services networks to implement domestic and international funds transfer transactions, be it business to business transfers, business to consumer transfers and vice versa, as well as consumer to consumer transfers. In particular, although not exclusively, the invention relates to a method and apparatus for effecting electronic funds transfers, akin to telegraphic transfers, which utilize a global public communications network (such as the "Internet") and business hubs for integrating with credit card settlement arrangements and financial networks utilised by financial institutions. Multiple currency transactions may also be accommodated by the electronic payment system of the invention.

(ii) Discussion of the Background Art

Existing arrangements for initiating funds transfers typically involve a business or consumer providing instructions to the financial institution via a branch, either in person or in writing, or directly via financial institution supplied proprietary work stations located in a business's offices. Manual preparation of instructions is slow and inefficient, whilst the cost for both the businesses, consumers and the financial institution for installation and maintenance of proprietary work stations can be prohibitive. The consumers and businesses encompass parties that wish to trade in goods and services, as well as anyone who may wish to remit funds to another party or, as the context may require, the relevant authorised signatories of those parties.

Currently, when financial institutions make cross border payments on behalf of a paying party ("payer"), that party's payment instruction is typically manually converted by the payer's financial institution into a message that is then sent to the recipient party's ("payee") financial institution. Such messages must generally be assembled in accordance with a specific protocol, such as SWIFT, that is generally recognised and accepted by banks and other financial institutions. If the payer's financial institution and the payee's financial institution do not maintain a relationship with one another, an

additional message must also be sent to the payer financial institution's correspondent financial institution.

The SWIFT financial network acts to route messages between member financial institutions, typically banks. Some validation of data is performed, however this validation does not usually include validation of information relating to the transaction, such as the payer account number with the payer's financial institution, as financial networks like SWIFT do not maintain such information. Member financial institutions settle against each other for individual transactions, if correspondent financial institutions are also involved, then multiple settlement "legs" are required. Settlement needs to be performed for each individual transaction, which adds to service costs and possible delays in transmission of funds.

When a financial institution wishes to offer a variety of foreign currency services, it must maintain individual relationships in each location for every currency they wish to offer. A foreign currency payer is also exposed to the risk of unfavourable exchange fluctuations when settlement occurs some days after payment is authorised.

BRIEF SUMMARY OF THE INVENTION

(i) Object of the Invention

It is an object of the present invention to provide an apparatus and method for effecting electronic funds transfers, akin to telegraphic transfers, but which delivers a more rapid and economical method of processing payments, when compared with traditional funds transfer arrangements.

It is another object of the invention to provide an apparatus and method for effecting electronic funds transfers which may be implemented quickly and conveniently through integration with existing financial networks, particularly networks and arrangements utilised for credit card settlement purposes.

It is a further object of the invention to provide an apparatus and method for effecting electronic funds transfers which may substantially reduce foreign exchange risks.

It is a still further object of the invention to provide an apparatus and method for effecting electronic funds transfers which allows remote, secure electronic initiation by

payers and which facilitates on-line tracking and reconciliation of payments.

It is a yet further object of the invention to provide an electronic funds transfer system which ameliorates and more appropriately shares the risks associated with undertaking financial transactions via the Internet.

(ii) Disclosure of the Invention

In a first form, relating to a typical commercial transaction, the invention resides in a method of effecting an electronic transfer of funds between a payer account and a payee account wherein the payer account and the payee account are each held by respective parties at financial institutions associated with a financial settlement network; said method including the steps of:

(a) a payer providing a purchase order to a payee, which purchase order identifies the payer to the payee;

(b) a payee, subsequent to receipt of the purchase order, providing an invoice to the payer, which invoice identifies the payee account for crediting funds in the transfer;

(c) the payer, in response to receipt of the invoice and subsequent to approval of the transfer, transmits a secured payment instruction to a payment gateway, which payment instruction identifies the payer account for debiting;

(d) the payment gateway, in response to receipt of the secured payment instruction and subsequent to ensuring authenticity of the payment instruction, creates a payment request message for the payer's financial institution and passes the payment request to the financial settlement network; and

(e) the payment gateway, in response to a payment authorisation message from the payer's financial institution, notifies payment approval to the payer and passes a settlement message to the financial settlement network, whereby the settlement network facilitates settlement of the transfer on a net basis with the payer's financial institution and the payee's financial institution.

Preferably the payer provides the purchase order to the payee by transmitting said purchase order via a business hub or business portal.

Preferably, the payee provides the invoice to the payer by transmitting said invoice via a business hub or business portal.

Suitably parties are each allocated a unique identifier that is registered with the

payment gateway.

The unique identifier for each party is desirably registered with the payment gateway in relation to a at least one account with a financial institution.

A party may register a merchant account for selling purposes and/or a debit account for purchasing purposes, as required.

Each debit account may be associated with at least one signatory registered with a trusted authority for security purposes.

Suitably financial institutions are each allocated a unique identifier that is registered with the payment gateway. In the case of a bank, a bank identification number (BIN) may form the financial institution identifier.

Preferably the purchase order includes the payer's identifier and a description of goods and/or services desired to be purchased.

Suitably the invoice includes the payee's identifier and the payee account is selected from a merchant account registered with the payment gateway.

Preferably the payer creates a payment instruction by accessing the business hub, selecting a payer account from the debit accounts registered with the payment gateway and indicating the currency and amount for payment.

The payer may select a foreign exchange rate from a board rate specified by the financial institution.

An approved signatory desirably applies a security means to the payment instruction prior to transmission to the payment gateway.

Suitably payers maintain a signing matrix of approved signatories on the payment gateway for each registered debit account.

Preferably the payment gateway ensures authenticity of the payment instruction by checking the security means against the approved signatories for the registered debit account.

The payment request is preferably created by reformatting the information

contained in the payment instruction, including the payer account ar identifier corresponding to the payer's financial institution.

The payment request may be an SMS 0200 financial transaction req message sent to the financial network which includes a credit card settlement networ

In preference, the financial network transmits settlement messages to financi institutions at least daily.

The settlement message may be a Base II settlement message.

Upon settlement, the payer and optionally the payee, may be notified of the funds transfer.

Most preferably, the financial network settles the payment transaction on a net basis for both domestic and international transactions, through at least one settlement financial institution.

An agent financial institution will facilitate foreign currency settlement with the payer's financial institution and/or the payee's financial institution, as required.

In another form, suitable for electronic commerce, the invention resides in an electronic funds transfer apparatus for effecting transfer of funds between a payer account and a payee account wherein the payer account and the payee account are held by respective parties at financial institutions that are associated with a financial settlement network, said apparatus comprising:

(a) a payment gateway having a payment web server and a payment factory, wherein the payment web server communicates with the parties, and the payment factory communicates with a plurality of financial institutions;

(b) the payment web server is operative to provide payment services to parties, wherein payers transmit secured payment instructions to the payment gateway subsequent to receipt of invoices from payees, which invoices identify the payee account for crediting in the transfer; and

(c) the payment factory is operative to process said secured payment instructions, which instructions identify the payer account for debiting, by creating messages for the financial settlement network requesting authorisation of payment from the payer account and initiating settlement of the transfer on a net basis with respective financial institutions of the payer and the payee.

Preferably the payment web server includes an integrated module for offering payment services to payers and payees via at least one business hub or business portal.

Suitably the invoices are transmitted by payees to payers via said at least one business hub or business portal.

Most preferably the payment web server includes a payment security arrangement for securing information supplied to said at least one business hub or business portal.

Suitably the payment security arrangement includes a security proxy for securing information identifying the payer account, the payee account and the funds for transfer.

Preferably the payment factory includes an administration module for registering parties that wish to effect funds transfers by allocating a unique identifier to each party.

Most preferably the payment factory includes a payment engine for processing the secured payment instructions and creating messages formatted for the financial settlement network.

Preferably the payment web server communicates with said at least one business hub and with said hubs and portals and with registered parties via a public communications network, such as the Internet.

Preferably the payment factory further includes interface means for communicating the authorisation request messages and settlement messages to the financial institutions via the financial settlement network.

Suitably the financial settlement network includes credit card networks.

Preferably the payment factory further includes a security server for authenticating communications using predetermined securing means.

Suitably the predetermined securing means for communicating via the public communications network include digital certificates and private keys allocated to

contained in the payment instruction, including the payer account and an identifier corresponding to the payer's financial institution.

The payment request may be an SMS 0200 financial transaction request message sent to the financial network which includes a credit card settlement network.

In preference, the financial network transmits settlement messages to financial institutions at least daily.

The settlement message may be a Base II settlement message.

Upon settlement, the payer and optionally the payee, may be notified of the funds transfer.

Most preferably, the financial network settles the payment transaction on a net basis for both domestic and international transactions, through at least one settlement financial institution.

An agent financial institution will facilitate foreign currency settlement with the payer's financial institution and/or the payee's financial institution, as required.

In another form, suitable for electronic commerce, the invention resides in an electronic funds transfer apparatus for effecting transfer of funds between a payer account and a payee account wherein the payer account and the payee account are held by respective parties at financial institutions that are associated with a financial settlement network, said apparatus comprising:

(a) a payment gateway having a payment web server and a payment factory, wherein the payment web server communicates with the parties, and the payment factory communicates with a plurality of financial institutions;

(b) the payment web server is operative to provide payment services to parties, wherein payers transmit secured payment instructions to the payment gateway subsequent to receipt of invoices from payees, which invoices identify the payee account for crediting in the transfer; and

(c) the payment factory is operative to process said secured payment instructions, which instructions identify the payer account for debiting, by creating messages for the financial settlement network requesting authorisation of payment from the payer account and initiating settlement of the transfer on a net basis with respective financial institutions of the payer and the payee.

Preferably the payment web server includes an integrated module for offering payment services to payers and payees via at least one business hub or business portal.

Suitably the invoices are transmitted by payees to payers via said at least one business hub or business portal.

Most preferably the payment web server includes a payment security arrangement for securing information supplied to said at least one business hub or business portal.

Suitably the payment security arrangement includes a security proxy for securing information identifying the payer account, the payee account and the funds for transfer.

Preferably the payment factory includes an administration module for registering parties that wish to effect funds transfers by allocating a unique identifier to each party.

Most preferably the payment factory includes a payment engine for processing the secured payment instructions and creating messages formatted for the financial settlement network.

Preferably the payment web server communicates with said at least one business hub and with said hubs and portals and with registered parties via a public communications network, such as the Internet.

Preferably the payment factory further includes interface means for communicating the authorisation request messages and settlement messages to the financial institutions via the financial settlement network.

Suitably the financial settlement network includes credit card networks.

Preferably the payment factory further includes a security server for authenticating communications using predetermined securing means.

Suitably the predetermined securing means for communicating via the public communications network include digital certificates and private keys allocated to

registered parties by a trusted authority, such as a certification authority.

Desirably, the financial settlement network transmits settlement messages at least daily to financial institutions in the network.

The electronic funds system of the invention provides several advantages over prior art payment systems such as SWIFT. The party registration process reduces error rates when creating and receiving payments because the system can perform party validation up-front as each transaction is created. This validation is reinforced by the financial institution authorisation messages that are obtained when each payment instruction is approved. Thus lower error rates, which call for repairs in the prior art systems, results in lower processing costs for the system of the invention.

The invention also provides a direct interface for parties of all financial institutions in the credit card settlement network. The financial institutions do not need to spend money and expend resources to develop proprietary work stations to support parties.

Parties can operate different accounts with their different financial institutions through one web application, and there will be economies of scale if a majority of associated financial institutions adopt the system. Party set up and maintenance costs to financial institutions of the web application is lower compared with financial institution proprietary systems.

Payer payment instructions are converted by the system into a settlement message that can be carried over the credit card network. No manual effort is required by financial institutions which results in further cost savings. The credit card network conveniently provides routing and processing for business to business transactions.

Many financial institutions already have the necessary infrastructure to support credit card networks. Financial institutions may settle on a net basis instead of on a per transaction basis, which allows lower balances to be maintained with settlement financial institutions.

Financial institutions require a relationship with one domestic or national settlement (NNS) financial institution and with one international settlement (INS) financial institution. Credit card networks have an established base of financial institutions together with business and individual consumers, thus providing economies

of scale.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing the objects involved in an electronic funds transfer in accordance with a first embodiment of the invention;

FIG. 2 is a diagram illustrating the steps in a method of electronic funds transfer of the first embodiment;

FIG. 3 is a diagram depicting the electronic funds transfer apparatus of the first embodiment;

FIG. 4 is a diagram illustrating security arrangements for the electronic transfer system of the first embodiment; and

FIGS. 5A and 5B are diagrams, that together, illustrate details of the architecture of an electronic funds transfer apparatus of a second embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The diagram in FIG. 1 illustrates one example of the entities and components involved in the operations of the electronic funds transfer system 100 of a first embodiment of the invention. In the example there is a payer 101, such as a buyer, that wishes to acquire certain goods or services and a payee 102, such as a seller, that is offering goods and services for sale. Payers and payees may be introduced to one another by way of a business hub or business portal 103, which is associated with a payment gateway 104. In the example, the portal 103 allows businesses to offer goods and services for direct electronic ordering by other businesses who have certain requirements and have utilised the portal to search for and obtain details of the required goods/services.

The payer 101 and payee 102 are able to communicate with the portal 103 and the payment gateway 104 via a public communications network 109, such as the Internet. The system 100 will typically allow for additional business portals 105 and 106, which like portal 103, will communicate with the payment gateway 104 via the Internet. Whilst only one payer and one payee is shown in the diagram for reasons of clarity, it will be appreciated that such business portals or hubs will each provide

facilities allowing many payees to interact with many more potential payers. The portals may be aligned with certain related business sectors for example.

The payment gateway 104 provides an interface into a financial settlement network 105, here a credit card network, which utilizes certain communications protocols to link a payer financial institution, such as payer bank 106, a payee financial institution, such as payee bank 107 and an agent financial institution, such as agent bank 108. In the embodiment, the financial network includes a private secure communications network linking member financial institutions that is maintained for the purposes of credit card transactions, such as VISANET. Again only the payer bank 106 (of payer 101) and the payee bank 107 (of payee 102) are illustrated, although many financial institutions will be members of the relevant credit card association. In other embodiments, the payment gateway processing capability, or selected modules of that capability, may be situated at a selected financial institution.

In order to use the electronic funds transfer system 100 of the embodiment, each party may be set-up with a profile which is unique for each party, irrespective of whether the party is a payer 101 or a payee 102, or both. This will at least include details of a payer account 111, whereas a payee account 112 may be included as required. Parties which are business entities may also establish user groups in order to define functionality access and data access rights to the system for individual users within the business entity. Each business party may also have access to multiple accounts from multiple financial institutions, thus financial institution accounts are mapped to specific parties. Accordingly, set up procedures also involve, for the parties that are business entities, designating signatories and assigning each account to an approved signatory.

In one arrangement, payer accounts are associated with a signing matrix wherein signing authorities of parties that are business entities are assigned to specific access levels within the funds transfer system. Digital signatures, which are specific to an individual, whether a payer or employee of a payer business entity, are issued to account signing authorities. The digital signatures issued to individuals are useable with multiple accounts, but are typically financial institution specific. Individual users can then activate their digital signatures through a trusted certificate authority 110. Suitably, each party is made responsible for all party internal security matters. Authorised signatories of the electronic system will perform due diligence checks during processing (as explained further below). However, liability for pre-processing fraud in this arrangement is typically borne by the payer.

In order to set up arrangements the financial institutions need to establish card accounts for each payer, assigning the card account numbers to the payer. Similarly, a common, trusted certificate authority should be agreed by the financial institutions. The trusted authority 110 will desirably be independent, external and will bear liability for registration and identification of signing authorities, through a security arrangement such as a digital signature mechanism. A database associated with the payment gateway 104 stores necessary party, account and financial institution information, as will be described in further detail herein below.

A method of effecting electronic funds transfer of the first embodiment will now be described in relation to FIG. 2. In the embodiment the payer party will have been registered with the payment gateway 104. The payer 101 has, in this example, previously logged onto a business hub, such as business to business (B2B) portal 103, through the Internet and has decided to purchase certain goods or services offered by payee 102. The payer 101 sends a purchase order 200 to the payee via the B2B portal 103. In response to receipt of the purchase order, the payee 102 creates an invoice 201 which identifies a payee account for 112 crediting of funds for the purchase. The account is suitably chosen from a list of payee accounts registered with the gateway 104, thus eliminating the possibility of incorrect account information which might delay settlement. The invoice is sent to the payer via the B2B portal 103. It will be appreciated that purchase orders and invoices may be provided, in other variants of the invention, on paper by mail or perhaps communicated verbally by telephone.

Upon receipt of the invoice 201, the payer 101 or an appropriate signatory in the payer business organisation, checks and approves the purchase by creating a payment instruction 202. The payer will select which currency and account number to make the payment from, before the invoice is preferably batched with others for approval. The B2B portal may also allow the payer, or managers or other signatories of payers that are business entities to log on via the payment gateway to review and separately approve payments on an individual or batch basis. The payer can also set up rules for foreign exchange rate to be either taken from the prevailing board rate or to request a treasury quote.

Although the payer continues to interact with the B2B portal 103, the payment instruction, when complete, is transmitted to the payment gateway 104 together with information identifying the payee and the transaction. The information with the payment instruction, which is encrypted and digitally signed by the payer, suitably

includes the payee's name, account number, invoice number, purchase order number, payment amount and currency, as supplied by the B2B portal 103. It should be noted that for payers that are business entities, there may be multiple signatories which can be accommodated by the signing matrix described below.

The payment gateway 104 decrypts the payment instruction 202 and checks the instruction against the payer's signing matrix. This suitably involves authentication 203 with the trusted certificate authority 110. If the digital signature is authenticated, the payment instruction 202 is immediately reformatted into a payment authorization request message 204 suitable for the financial network 105. In the method of the embodiment, a Base I 0100 message containing the payer (issuing) financial institution ID is created and passed to VISANET network. In an alternative arrangement, an SMS 0200 message may be created.

The financial network 105 then routes the payment request message 204 to the payer bank 106. The payer bank will check for available balance before returning a payment authorisation message 205, such as a Base I 0110 message or an SMS 210 message, via the financial network 105 to the payment gateway 104.

The payment gateway 104 will re-format the payment authorization message and update the B2B portal information about the transaction, for example the payment authorization code provided with the 0110 (or alternatively SMS 0210) response may be appended to the payment request, to enable payer and payee to view the status of the payment through the Internet. The payment gateway 104 will send a payer notification 206a to the payer that the payment has been approved through the B2B portal or directly via the Internet. Payers 101 can be notified either on a real time or on a batch basis. The payment gateway can, if required, provide additional data to enable the payer to update their enterprise resource planning (ERP) or corporate host system.

Similarly, the payment gateway 104 will send a payee notification 206b to the payee 102 that the payment has been approved through the B2B portal or the Internet. The payees can be notified on a real-time or batch basis. The gateway may again provide data to enable the payee to update their ERP or corporate host system, as required.

On at least a daily basis, the credit card settlement network, VISANET in the example, will settle the transactions on a net basis for domestic and international transactions. An agent financial institution 108, such as a major international bank,

will effect financial settlements with the VISA member financial institutions on behalf of VISA.

An overview diagram of an electronic funds transfer apparatus 300 of a first embodiment of the invention is illustrated in FIG. 3. The apparatus comprises a payment gateway 301, which communicates with exemplary trusted certificate authority systems 302, consumer/business (party) computer systems 303, and business hubs 304 via the Internet 305. The payment gateway 301 also communicates with financial institution computer installations via financial networks, including the VISANET network 306 and the value added network (VAN) 307. The exemplary financial system installations include those for a issuing bank 308 and for an acquirer bank 309.

The payment gateway 301 incorporates a payment web server 310 which hosts the web front end to all services offered by the system of the embodiment, including the core payment service and other value added services. The functions provided by the web server 310 include:

- supporting payer initiation of payment and entry of payment instruction information, with batch payment for payer if required;
- supporting multi-authorisation matrix signing for payers that are business entities;
- allowing a payer to select from a list of pre-registered paying financial institution and accounts for payment;
- allowing a payee to indicate through the B2B hub the crediting account from a list of pre-registered acquiring financial institution and accounts;
- supporting secured inquiry and report down-load for payer and merchant through the Internet; and
- inquiry and down-load of system reports on periodic or upon-request basis for merchants, payers, e-commerce hubs and financial institutions, including reports on approved payments, declined payments, exceptions, transaction details, transactions summary.

The payment web server 310 also includes an integration module 311 for embedding of pages in the business to business (B2B) hubs 304. This module offers web pages, applets to offer payment services through the B2B hub web front end. The web services though hosted on the payment web server 310 can be integrated into a B2B hub's web pages 312 giving a consistent look and feel. This will allow B2B hubs to offer an electronic funds transfer payment service quickly and with minimum

integration effort. The integrated module 311 also includes a payment security proxy sub-module 313 to encrypt sensitive information such as account number at the point of data entry. Such encrypted confidential information may suitably only be decrypted by an integration package at the issuing financial institution. This assures the privacy of the confidential information during transmission and storage of data between the point of entry to the point where the information is required.

The payment gateway 301 also includes a payment factory 314 that is the processing module of all electronic funds transfer services and functions. The payment factory has several sub-modules including a security server 315, a payment engine 316, a payment log 317, an administration sub-module 318, a "value added services" sub-module 319, along with a VISANET interface 320 and a value added network (VAN) interface 321 for the respective networks.

The security server 315 provides digital certificate authentication for point to point connections between the payment gateway 301, B2B hubs 304 and issuing financial institutions 308; digital certificate authentication for payer parties; and cryptographic services to decrypt the data passed from payer entry, including payer ID, invoice number, amount, issuing financial institution, payer account number, acquiring financial institution and payee account number.

The payment engine 316 this module carries out all payment related processing. The payment engine manages payer authentication flow, issuing authentication requests through VISANET or initiate the authentication processing function within the engine. The payment engine manages payment message flow, including the sequence and state of payment message processing, initiation and routing. Payment message formatting is also handled by the payment engine, including payment message interpretation and initiating responses to parties. The payment engine manages a signing-matrix database and performs signing-matrix verification.

The payment log sub-module 317 logs all payment activities including payer inputs, payment messages and response to parties 303 for accounting and tracing purposes. The administration sub-module 318 handles both registration and profile configuration for payers and payee (or merchant) registration and profile configuration. Application administration for payment gateway operators (such as banks and other financial institutions) is also facilitated, including user access, administration, security configuration and similar "house keeping" functions for operators. The logging of administration activities of payers, merchants, and operators is also conducted.

The value added services sub-module 319 provides a variety of inquiry and reporting functions including payment inquiry, summary and detailed payment reports for payers and merchants, AR and AP reconciliation, enterprise resource planning (ERP) integration, loyalty points scheme management and consumer profiling.

The VISANET interface 320 and VAN interface 321 each implement message formatting and protocol handling for the respective financial network communications systems.

Each of the installations for the financial institutions 308, 309 preferably include a payment service enhancement package 322. This package provides easy adoption of electronic funds transfer payment services with minimum development requirement and short service launch time for issuing financial institutions 308 and for acquiring financial institutions 309. The payment service enhancement package 322 integrates with existing financial institution system back-end 323 to suitably provide a turnkey solution for payer authentication, message transport and value added service operations.

It is anticipated that financial institutions will be responsible for setting up their consumers on the payment gateway 301 to provide the electronic funds transfer service. A party profile is established for each party by using the administration sub-module 318 to store party information and acquire a unique Party ID. Existing party accounts, credit card accounts in the embodiment, are then mapped to the party ID. The payment gateway also generates a User-Admin ID allowing the party to perform user administration. The security sever 315 is then employed to set up a signing matrix for each account and digital signatures for party approved signatories are mapped to specific accounts. Typically, the financial institution would forward a electronic funds transfer service package containing all relevant components to each party.

In turn, certain set up actions on the payment gateway 301 must then be undertaken by the party on receipt of the package from their financial institution. Individual user profiles are generated for payer personnel who are to have access to the payment gateway 301. Individual users are preferably assigned to user groups consistent with their functional responsibilities in the payer business organisation. Authorised signatories must activate their digital signatures through the appropriate trusted certificate authority 302. A party that is a business entity may establish a hierarchy of signatories for transaction initiation, which is preferably matrix based.

Each signing authority matrix is assigned to a specific account number. Typically, a business party would have three groups of signatories and, on average, two signatures required. Consider a notional account which may be operated from signatories from three user groups A, B and C as depicted in Table 1 below:

Account Number			
Group	A	B	C
self	10	20	30
A	40	50	60
B		70	80
C			90

Table 1 - Signing Matrix

An individual from user group A of the account can sign for up to 10 by themselves, up to 40 with another member of group A assigned to the same account, up to 60 with a member from group C assigned to the account, ... etc, as illustrated above. The signing of electronic transactions need not be dependent on corporate and account mandates held at the financial institution. Separate arrangements may be defined in electronic business (EB) agreements that are accepted by the company governance board.

Looking at the party end of the electronic funds transfer system 300, a business portal function is provided through the web pages 311 embedded in the business hubs 304. The portal functions include facilitating creation of invoices by a payee and facilitating payment by a payer. Party computer systems 303 access the B2B hubs 304 via the Internet 305 using a conventional web browser 324, such as Microsoft's Internet Explorer™ or Netscape's Navigator™. The party browser will suitably include a smart card plug-in component 325, since it is desirable that the certificates and private key issued by the trusted CA 102 to authorised signatories are stored on a smart card.

The principle security concerns of the electronic funds transfer system 300 in its operation are desirably:

- ensuring the confidentiality of data transmission,
- authenticating all parties involved in each transaction, and
- ensuring integrity of data in transactions;

when operating in the context of a world wide distributed environment, using the

Internet and web based applications with external party connections including financial networks (such as VISANET), business hubs and financial institutions (banks, etc.) The authenticity of Payee to Payment System and the authenticity of the Payer to the Payee are the responsibility of the B2B hub in the present embodiment. The B2B hub identifies the merchants with whom the payer can securely conduct electronic commerce. The merchant registration process eliminates the need for merchant authentication. Registration with the electronic funds transfer system ensures that the merchant has a relationship with a financial institution allowing it to receive electronic payments.

When the B2B hub web application 312 initiates the payment service, the Payer ID, Payee ID, Invoice Information and the B2B hub's Digital Signature are passed to the payment gateway 301. The B2B application, using the B2B hub private key, signs this data followed by encryption through a virtual private network (VPN) tunnel. This ensures the data confidentiality and integrity during transmission. Encryption using B2B hub's private key also ensures non-repudiation of the information transmitted. The payment gateway system will decrypt the data and authenticate the B2B hub using the enclosed digital certificate with a trusted CA.

When the payer completes and submit the payment instruction, the payment instruction details, and SHA1 hash will be encrypted using the payer's private key. The payer's digital certificate and the payer's private key are stored on the smart card held by the payer. This will ensure the non-repudiation of the payment instruction as well as the integrity of the data. The encrypted packet will be transmitted to the payment gateway 301 through the Internet 305 using SSL to ensure confidentiality. The security server 315 in the payment gateway will decrypt the data.

The security server 315 will authenticate the Payer with an appropriate authentication authority. The authentication authority may be the issuing financial institution 308, the payment gateway 301 or a trusted Certification Authority (CA) 302. Accordingly, the electronic funds transfer system 300 ensures confidentiality and integrity of payment data through each and every leg of data transmission involving the payment system. Each piece of data is accessible only by the necessary party. For example, the Payer's account information will only be known by the payment gateway, Payer's financial institution, Payee's financial institution, but not by the Payee or the B2B hub.

The electronic funds transfer system 300 can implement a variety of currently

available protection schemes that are compliant with communications industry standards. The standards which the system can be configured to comply with include 168 bit Triple-DES, 1024 bit RSA, MD5, SHA1, X.509, 128 bit SSL v.3 and IPSec. Further details of these schemes can be obtained from the relevant standards documents.

The security deployment arrangements suitable for use with the first embodiment of the invention are now described in relation to FIG. 4, as follows. The security schemes may be implemented with a security toolkits such as Baltimore J/PKI+, which secures the following communication points as illustrated in the drawing. The User to Trading Hub link 1 involves parties or "users" 401 logging into hubs 402 to view catalogues, send purchase requests, create invoices, and to make payment requests. Trading hubs 402 need to authenticate a users identity either using a Digital Certificate or User ID and password. The basic password rules need to be enforced. A secure sockets layer (SSL) link with 128-bit encryption would be used to maintain the confidentiality transportation of information only when required. There is no need to increase load by encrypting catalogues, unless necessary. Users 401 have to sign on orders and invoices using their own digital signature.

The User to Payment Gateway link 2 involves transport of payment instructions containing financial information. The identity of trading hubs will be authenticated by the payment gateway using a digital certificate. Users 401 will have to digitally sign on the payment instruction using digital signature scheme which may be verified through the Trusted Certificate Authority (CA) 406. Java applets are used to sign data that would be transmitted. SSL v.3 would secure the transmission of the encrypted data to the payment gateway 403.

The Trading Hub to Payment Gateway link 3 involves communication of Payment notifications and payment approval. Hubs 402 and payment gateways 403 exchange digital certificates in the data message for authentication. Secure communications between both parties using end-to-end link encryption or virtual private networks (VPNs), together with hash functions if required.

The Payment Gateway to Payment Gateway link 4 involves Payment instructions containing financial information. Secure communications between both parties 403, 404 using end-to-end link encryption over leased line.

The Payment Gateway to Financial institutions link 5 involves Payment

instructions containing financial information. Secure communications between both parties using end-to-end link encryption or virtual private networks (VPNs), together with hash functions.

The Payment Gateway to Trusted CA link 6 involves fetching of public keys for decryption. This link has no security risks as public keys are public information.

The Payment Gateway to VISANET link 7 involves data containing VISA Base I and II messages. Authentication gateways would have Station IDs issued by VISA for identification. Secure communications with VISANET 407 is via the Visa access point (VAP) interface.

In order to assist further understanding of the invention, a schematic diagram of a second embodiment of the electronic funds transfer system of the invention is illustrated in FIGs 5A and 5B. The system 500 provides a highly reliable and predictable service for mission critical business to business payments. The operation will withstand high volume on-line transaction on a continuous 24x7x365 basis. The transaction processing volume capacity of the system of the second embodiment is estimated at 1.8 million per day. The web hit rate is estimated at 300K per day.

Given the high volume expectation of electronic funds transfer business and the dynamic of volume growth of Internet related operations, the main payment factory application component will be operated using a first farm of servers 510, such as 4 Sun Enterprise 4500 Servers with 14 CPUs, each with 30TB of storage capacity. The server farm 501 will be inter-connected using a high-speed switching hub with high bandwidth back plane and communicate with the database 502 and GSM-SMS/e-mail/fax channel servers 503 via a closed loop circuit 504.

Similarly a second farm of web servers 510, such as Sun Enterprise 450 Servers, can cater for the demands of Internet traffic, together with a wireless application protocol (WAP) server 511 which are coupled to the Internet via a pair of firewall servers 512 and a pair of high performance routers 513, such as those produced by Cisco. Also included is an e-mail server 514, a virtual private network (VPN) server 515, a certification authority server 516 (for use by financial institutions) and a key management server 517. The web server farm 510 is coupled to the payment factory server farm 501 by a further pair of firewall servers 508.

Financial institution host systems 520 may be coupled to the electronic funds transfer system 500 via service enhancement package systems 521 through a VPN gateway server and the Internet (see FIG 5A) or directly to the closed loop circuit 504 (see FIG. 5B), as required.

To ensure the system's ability to scale its system to match the capacity growth, two strategies are essential. First employing a platform with an upgrade path for higher processing and storage capacity, and secondly providing a server farm configuration supported with corresponding application architecture, application functions and database partition design. The application architecture and application functions design will support proper load balancing and co-ordination of function execution distributed on multiple servers accessing different partitioned database. The database is expected to be partitioned based on grouping of issuing financial institution.

A procedure for monitor the system performance and capacity usage to project future capacity requirement is desirable. The system will typically consist of a large number of interconnected capacity elements including processing elements, I/O elements, network elements and storage elements. The complexity of the overall system capacity model demand that a capacity planning and simulation tool be used. A highly automated system management and monitoring application is desirable to ensure efficient, reliable and consistent system operation to meet the high volume and mission critical demand of the systems operations.

The large number of processing and other system components employed by the system 500 dictates that automated system management and monitoring is important. A partial light out operation will be the goal. Cross border monitoring and management is required in view of the geographical distributed but tightly integrated operation facility that is required for a global payment service. A set of multiple system management and monitoring tools, such as Tivoli, may be used as the framework and central console for integrating the systems. A communications management tool, such as HP Openview supplied by Hewlett Packard Corporation, will be the central control and monitoring tool for the network components of the system of the embodiment.

Sun Management Server, BMC tools and a suite of component specific tools can cover management and monitoring of the rest of the system components including tools for Oracle 8i database, Sun's Solaris operating system, Web server, storage system, system security, job control, application, change management, network performance monitoring/management, application performance monitoring/management, and

availability management of applications and services. The monitoring tools can track the component and system performance against baseline, identify faults, and anticipate eminent failure. Tracking data, warning and alerts may be delivered to the relevant parties through e-mail via the corporate e-mail gateway 505, paging/SMS 506 and facsimile 507. The automation will allow operators of the system to pre-empt problems and recover from failures in the shortest possible time.

Although an illustrative embodiment of the present invention, and various modifications thereof, have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to this precise embodiment and the described modifications, and that various changes and further modifications may be effected therein by one skilled in the art without departing from the scope or spirit of the invention as defined in the appended claims.

CLAIMS

1. A method of effecting an electronic transfer of funds between a payer account and a payee account wherein the payer account and the payee account are each held by respective parties at financial institutions associated with a financial settlement network, said method including the steps of:

(a) a payer providing a purchase order to a payee, which purchase order identifies the payer to the payee;

(b) a payee, subsequent to receipt of the purchase order, providing an invoice to the payer, which invoice identifies the payee account for crediting funds in the transfer;

(c) the payer, in response to receipt of the invoice and subsequent to approval of the transfer, transmits a secured payment instruction to a payment gateway, which payment instruction identifies the payer account for debiting;

(d) the payment gateway, in response to receipt of the secured payment instruction and subsequent to ensuring authenticity of the payment instruction, creates a payment request message for the payer's financial institution and passes the payment request to the financial settlement network; and

(e) the payment gateway, in response to a payment authorisation message from the payer's financial institution, notifies payment approval to the payer and passes a settlement message to the financial settlement network, whereby the settlement network facilitates settlement of the funds transfer on a net basis with the payer's financial institution and the payee's financial institution.

2. The method of claim 1 wherein the payer transmits the purchase order to the payee via a business hub.

3. The method of claim 1 wherein the payee transmits the invoice to the payer via a business hub.

4. The method of claim 1 wherein parties are each allocated a unique identifier that is registered with the payment gateway.

5. The method of claim 4 wherein the unique identifier for a party is desirably registered with the payment gateway in relation to at least one account with a financial institution.

6. The method of claim 5 wherein a party may register a merchant account for selling purposes and/or a debit account for buying purposes.

7. The method of claim 6 wherein the debit account is associated with at least one signatory registered with a trusted authority for security purposes.

8. The method of claim 1 wherein financial institutions are each allocated a unique identifier that is registered with the payment gateway.

9. The method of claim 4 wherein the purchase order includes the payer's party identifier and a description of the goods and/or services desired to be purchased.

10. The method of claim 6 wherein the payer creates a payment instruction by accessing a business hub, selecting the payer account from the debit accounts registered with the payment gateway and selecting the desired currency and amount for payment.

11. The method of claim 10 wherein, in the case of a foreign currency payment, the payer selects a foreign exchange rate from a board rate specified by the financial institution.

12. The method of claim 7 wherein an approved signatory applies a security means to the payment instruction prior to transmission to the payment gateway.

13 The method of claim 12 wherein payers maintain a signing matrix of approved signatories on the payment gateway for each registered debit account.

14. The method of claim 13 wherein the step of ensuring authenticity of the payment instruction includes the payment gateway checking the security means against the approved signatories for the registered debit account.

15. The method of claim 1 wherein the payment request is created by reformatting the information contained in the payment instruction, including the payer account and an identifier corresponding to the payer's selected financial institution.

16 The method of claim 1 wherein the payment request is an SMS 0200 financial transaction request message that is sent to the financial settlement network which includes a credit card settlement network.

17. The method of claim 1 including the further step of:

(g) notifying the payer upon settlement of the transfer.

18. The method of claim 1 wherein the credit card settlement network facilitates settlement of the funds transfer on a net basis for both domestic and international transactions through a settlement financial institution.

19. The method of claim 1 wherein an agent financial institution facilitates foreign currency settlement with the payer's financial institution and/or the payee's financial institution.

20 An electronic funds transfer apparatus for effecting transfer of funds between a payer account and a payee account wherein the payer account and the payee account are each held by respective parties at financial institutions associated with a financial settlement network, said apparatus comprising:

(a) a payment gateway having a payment web server and a payment factory, wherein the payment web server communicates with the parties and the payment factory communicates with the financial settlement network;

(b) the payment web server is operative to provide payment services to parties, wherein payers transmit secured payment instructions to the payment gateway subsequent to receipt of invoices provided by payees, which invoices identify the payee account for crediting; and

(c) the payment factory is operative to process said secured payment instructions, which instructions identify the payer account for debiting, by creating messages for the credit card settlement network requesting authorisation of payment from the payer account and facilitating settlement of the funds transfer on a net basis with respective financial institutions of the payer and the payee.

21. The electronic funds transfer apparatus of claim 20 wherein the payment web server includes an integrated module for offering payment services to payers and payees via at least one business hub.

22 The electronic funds transfer apparatus of claim 21 wherein the invoices are transmitted by payees to payers via said at least one business hub.

23. The electronic funds transfer apparatus of claim 21 wherein the payment web server includes a security arrangement for securing information supplied to said at least one business hub.

24. The electronic funds transfer apparatus of claim 23 wherein the security arrangement includes a security proxy for securing information identifying the payer account, the payee account and the funds for transfer.

25. The electronic funds transfer apparatus of claim 20 wherein the payment factory includes an administration module for registering parties that wish to effect funds transfers, by allocating a unique identifier to each party.

26. The electronic funds transfer apparatus of claim 20 wherein the payment factory includes a payment engine for processing the secured payment instructions and creating messages formatted for the financial settlement network.

27. The electronic funds transfer apparatus of claim 21 wherein the payment web server communicates with said at least one business hub and with registered parties via a public communications network.

28. The electronic funds transfer apparatus of claim 20 wherein the payment factory further includes interface means for communicating the authorisation request messages and settlement messages to the financial institutions via the financial settlement network.

29. The electronic funds transfer apparatus of claim 23 wherein the financial settlement network includes credit card networks.

30. The electronic funds transfer apparatus of claim 20 wherein the payment factory further includes a security server for authenticating said communications using predetermined securing means.

31. The electronic funds transfer apparatus of claim 20 wherein the predetermined securing means for communicating via the public communications network includes digital certificates and private keys allocated by a trusted authority.

32. The electronic funds transfer apparatus of claim 20 wherein the financial settlement network transmits settlement messages at least daily to financial institutions in the network.

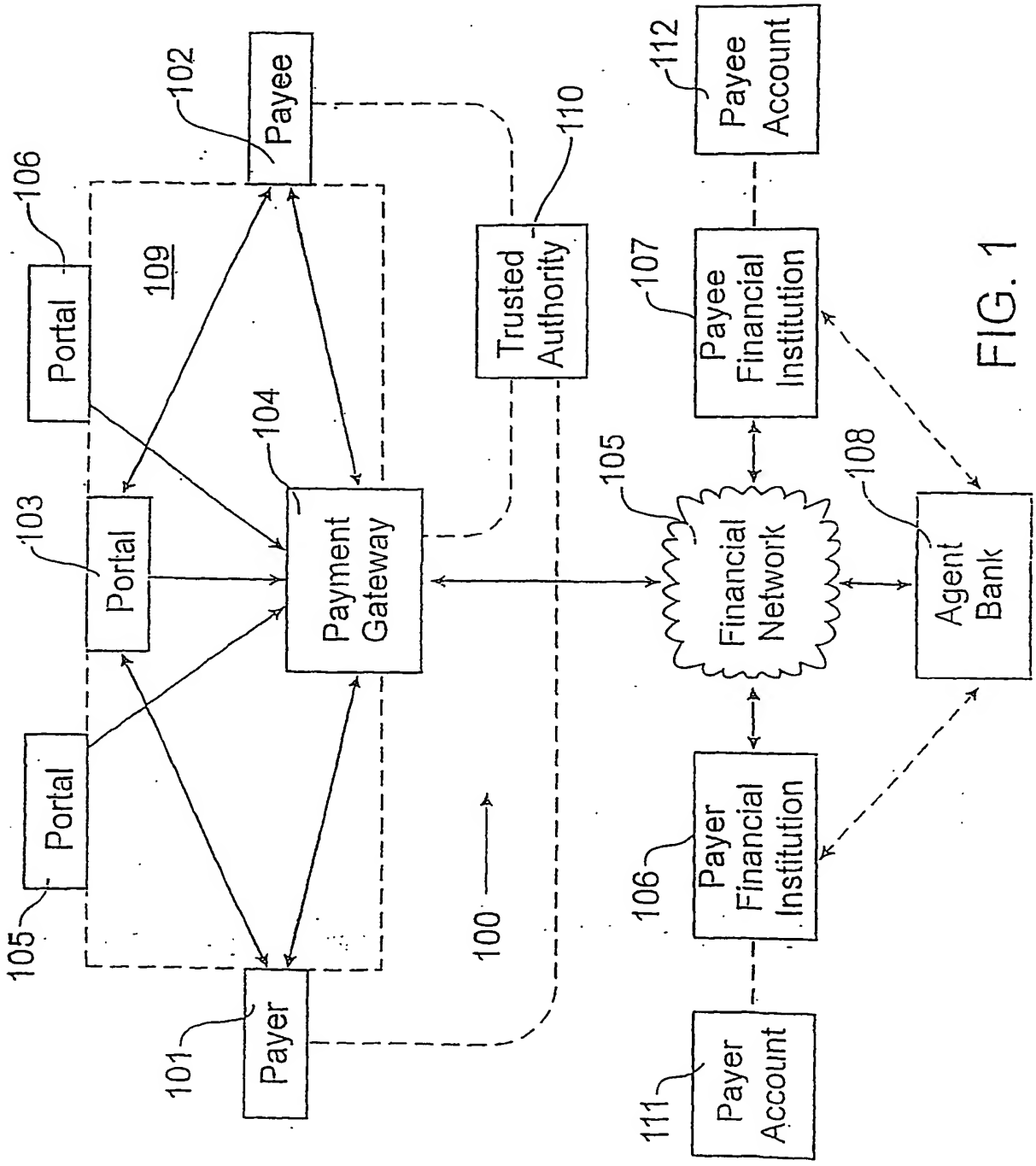

Payee
102
Payee Account
112
106
Portal
109
Trusted Authority
110
Payee Financial Institution
107
104
105
108
103
Portal
Payment Gateway
Financial Network
Agent Bank
Portal
105
100
106
Payer Financial Institution
101
Payer
111
Payer Account

FIG. 1

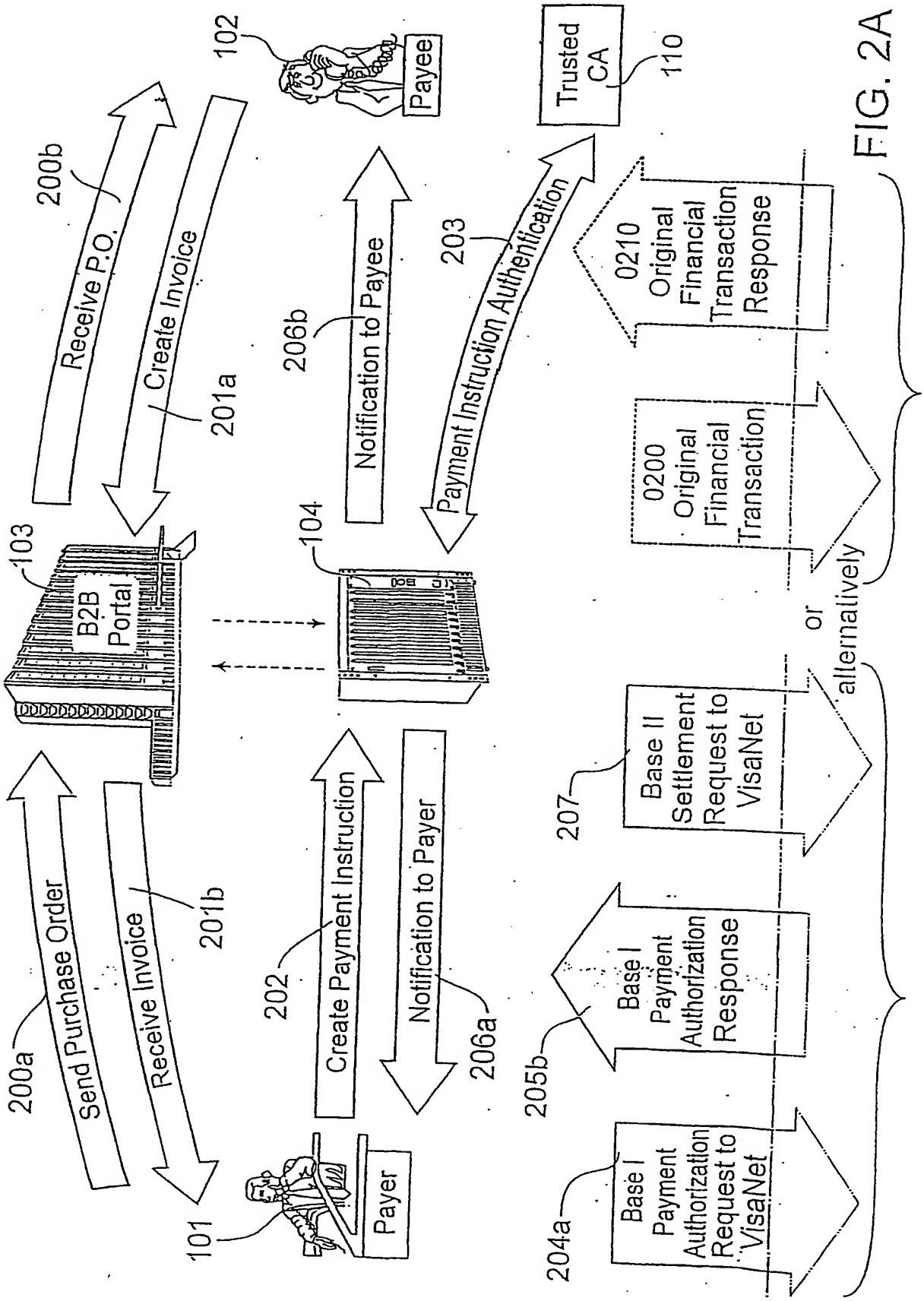

Payee
102
Trusted CA
110
200b
Receive P.O.
Create Invoice
201a
206b
Notification to Payee
203
Payment Instruction Authentication
0210 Original Financial Transaction Response
0200 Original Financial Transaction
or
alternatively
103
B2B Portal
104
200a
Send Purchase Order
Receive Invoice
201b
202
Create Payment Instruction
Notification to Payer
206a
207
Base II Settlement Request to VisaNet
205b
Base I Payment Authorization Response
204a
Base I Payment Authorization Request to VisaNet
101
Payer

FIG. 2A

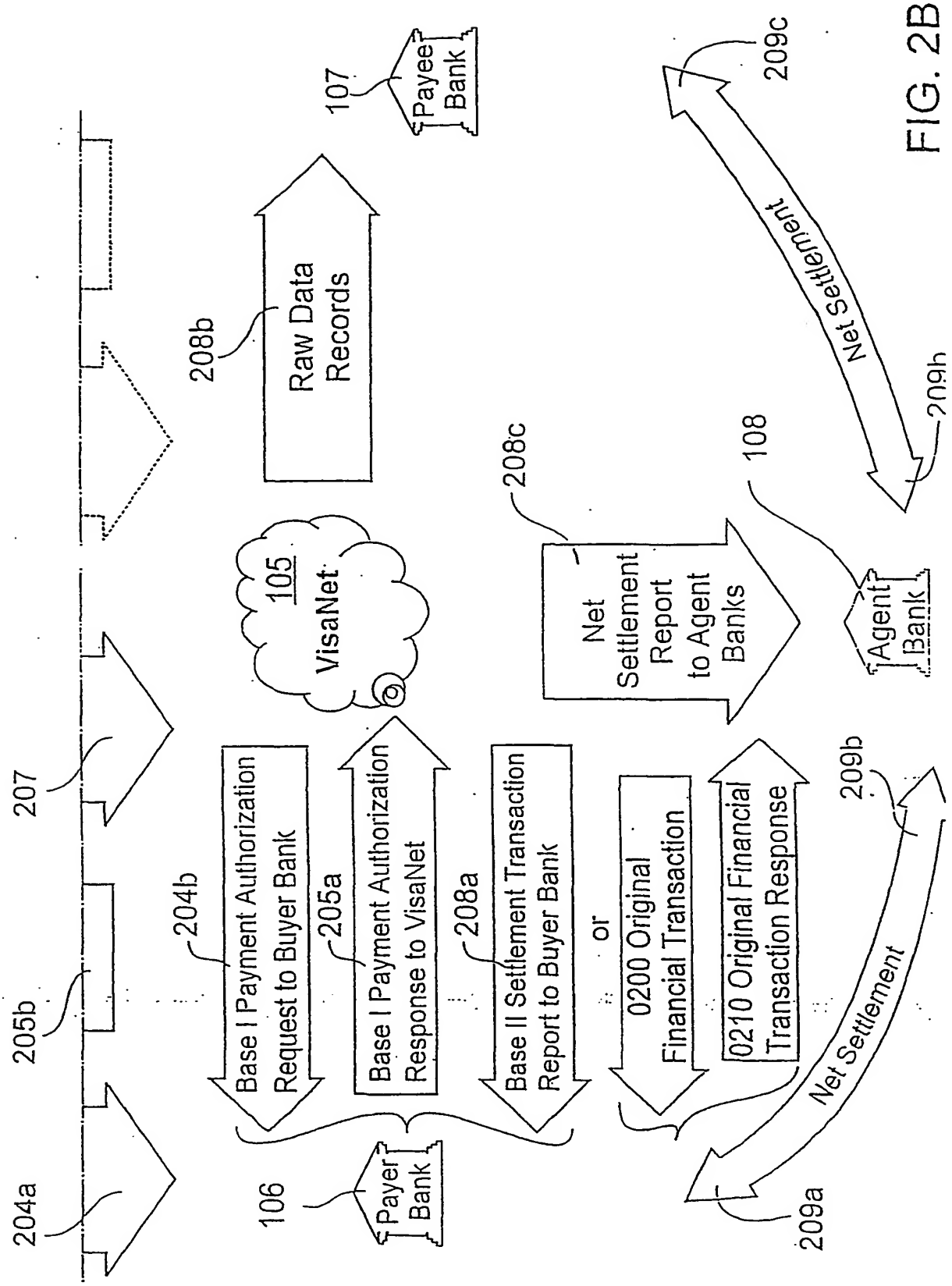

204a
205b
207
204b
Base I Payment Authorization Request to Buyer Bank
205a
Base I Payment Authorization Response to VisaNet
208a
Base II Settlement Transaction Report to Buyer Bank
or
0200 Original Financial Transaction
0210 Original Financial Transaction Response
106
Payer Bank
105
VisaNet
208b
Raw Data Records
107
Payee Bank
208c
Net Settlement Report to Agent Banks
108
Agent Bank
209a
Net Settlement
209b
Net Settlement
209c
209h

FIG. 2B

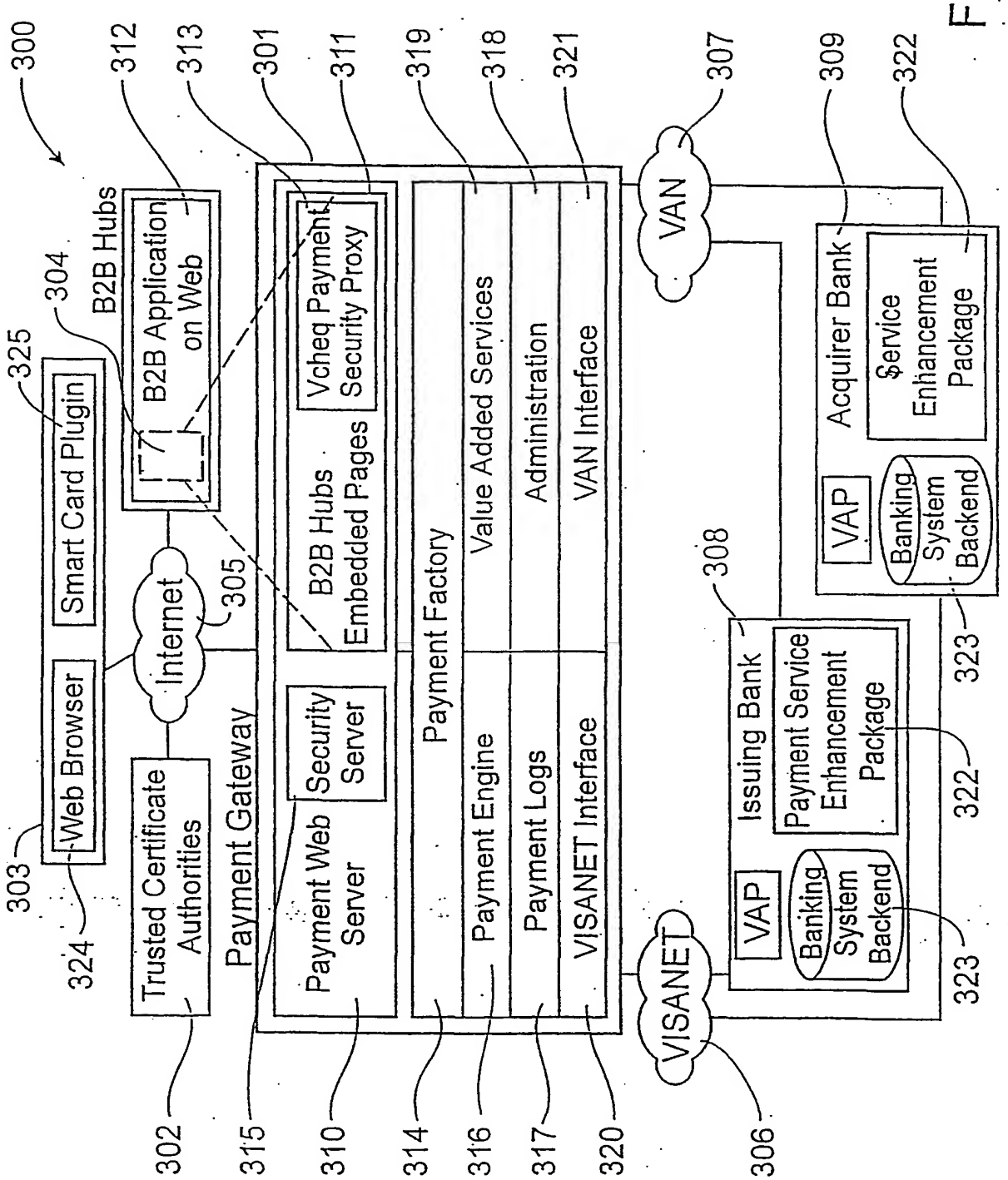

300
303
Web Browser
324
325
Smart Card Plugin
304
B2B Hubs
312
B2B Application on Web
313
Internet
305
Trusted Certificate Authorities
302
Payment Gateway
301
Payment Web Server
315
Security Server
310
B2B Hubs Embedded Pages
311
Vcheq Payment Security Proxy
319
Payment Factory
314
Payment Engine
316
Payment Logs
317
VISANET Interface
320
Value Added Services
318
Administration
321
VAN Interface
VISANET
306
VAN
307
Issuing Bank
308
VAP
Banking System Backend
323
Payment Service Enhancement Package
322
Acquirer Bank
309
VAP
Banking System Backend
323
$ervice Enhancement Package
322

FIG. 3

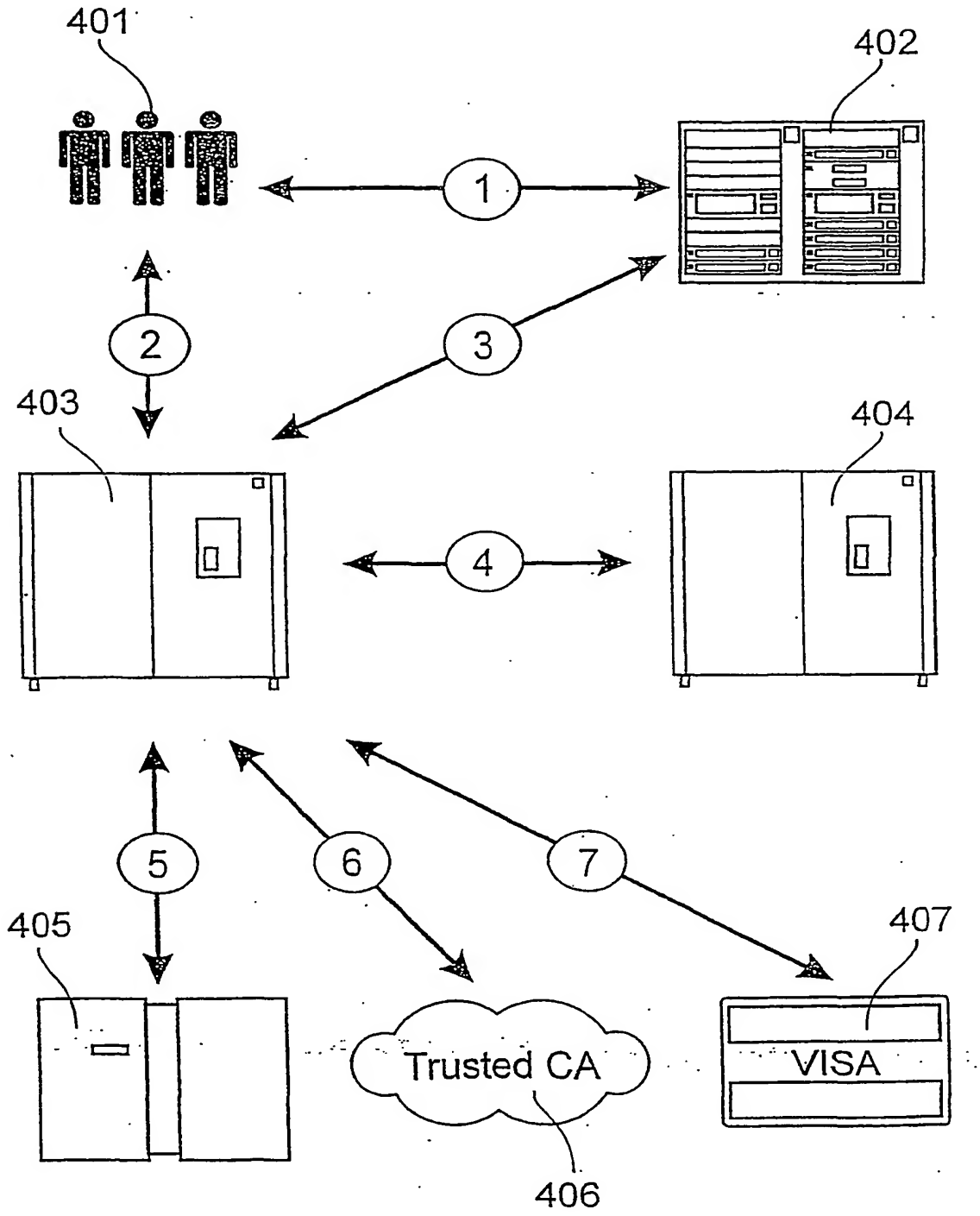


FIG. 4

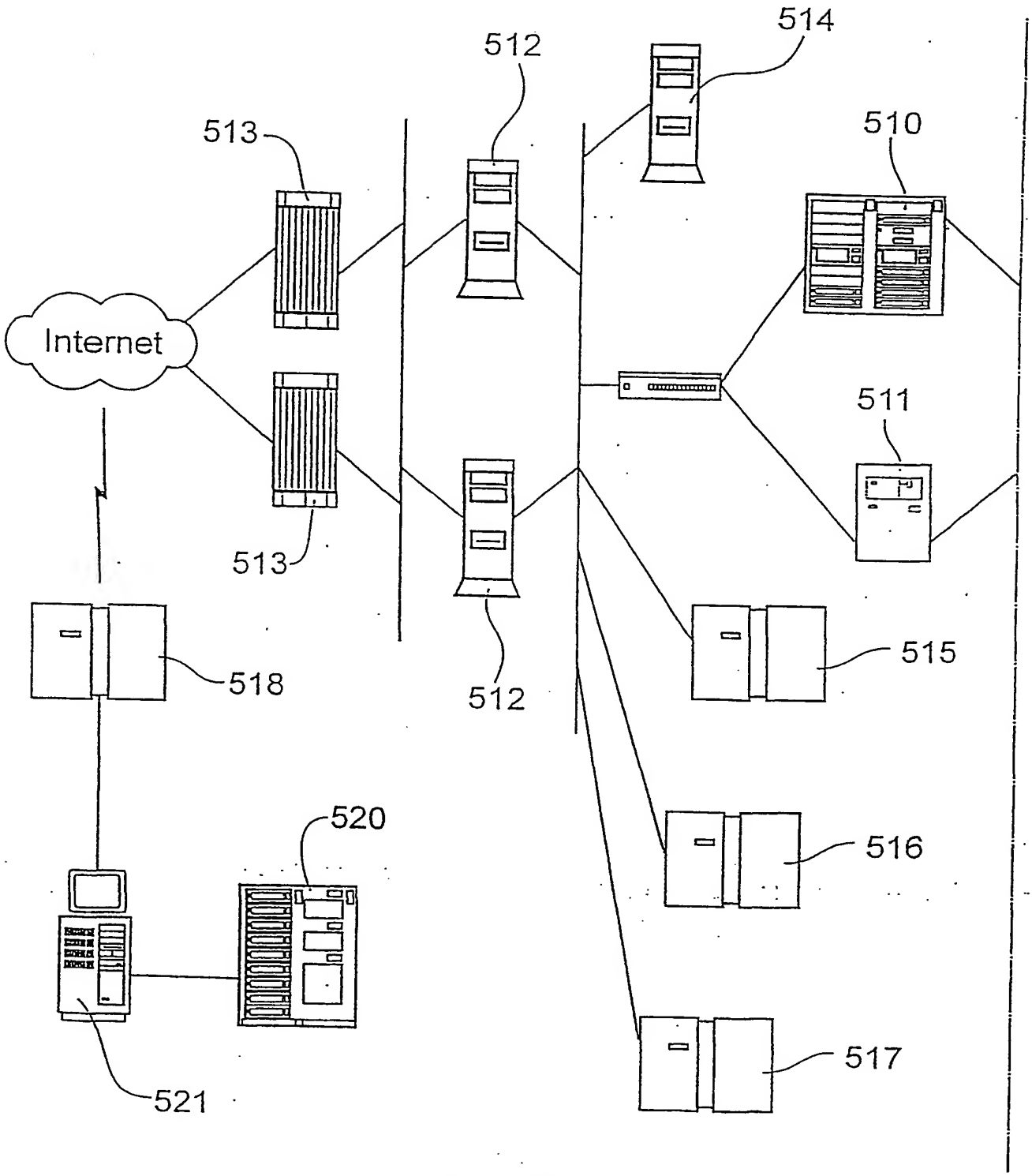


FIG. 5A

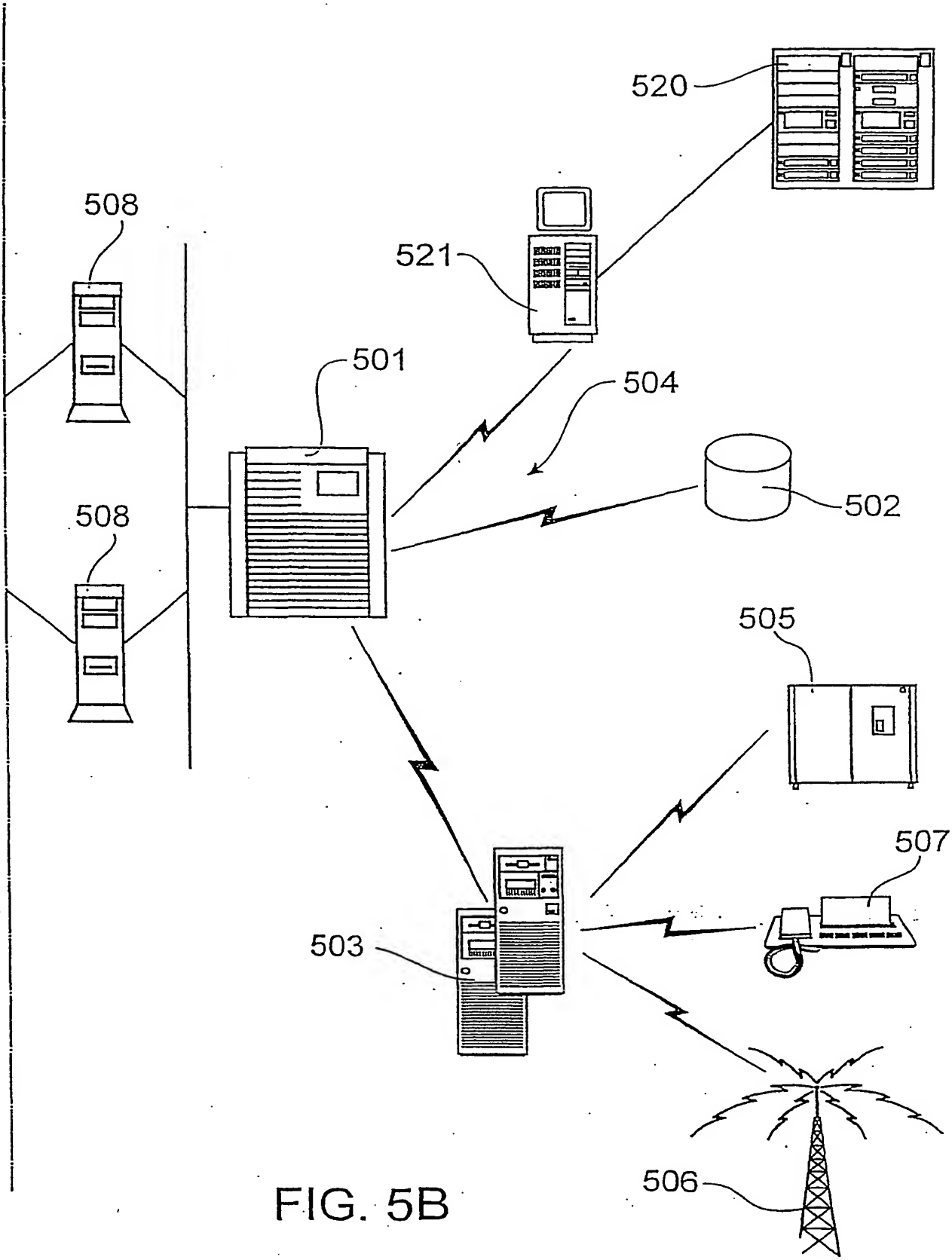


FIG. 5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 01/00153

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: G07F 19/00, G07F 7/10, G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: G07F, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	US 5677955 A (Doggett et al.), 14 October 1997 (14.10.97) *col. 5,7,8, col. 12, lines 49-50, fig. 3.* *col. 7,8, fig. 3.* *col. 7,8, fig. 3.*	1,7,9,12,17,18, 20,24,29 2,3,21,22,23,27 4-8,10,11,13-16,19,25,26,28,30-32
Y	GB 2251098 A (Allied Irish Banks PLC), 24 June 1992 (24.06.92) *(abstract). [online] [retrieved on 2001-09-25]. Retrieved from: EPOQUE WPI Database*	2,3,21,22,23,27
A	US 5920847 A (Kolling et al.), 6 July 1999 (06.07.99) *col. 11-13, col. 20, lines 60-68, fig. 8.* ----	1-32

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 October 2001 (01.10.2001)	21 November 2001 (21.11.2001)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer STEINZ Telephone No. 1/53424/387

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 01/00153

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
GB	A1	2251098	24-06-1992	GB	A0	9027301	06-02-1991
GB	B2	2251098	05-10-1994				
US	A	5677955	14-10-1997	BR	A	9608448	07-12-1999
				CA	AA	2217593	10-10-1996
				EP	A1	819345	21-01-1998
				JP	T2	11503541	26-03-1999
				WO	A1	9631965	10-10-1996
US	A	5920847	06-07-1999	AU	A1	80984/94	23-05-1995
				AU	B2	686270	05-02-1998
				BR	A	9407964	03-12-1996
				CA	AA	2175473	11-05-1995
				CA	AA	2175476	11-05-1995
				EP	A1	727072	21-08-1996
				EP	A4	727072	14-11-2001
				HU	A0	9601130	29-07-1996
				HU	A2	74351	30-12-1996
				HU	B	219257	28-03-2001
				JP	T2	9504634	06-05-1997
				JP	B2	2916543	05-07-1999
				KR	B1	237935	15-01-2000
				LT	A	96060	27-01-1997
				LT	B	4154	25-04-1997
				LV	A	11648	20-12-1996
				LV	B	11648	20-08-1997
				NO	A0	961707	29-04-1996
				NO	A	961707	25-06-1996
				NZ	A	275027	24-04-1997
				PL	A1	314309	02-09-1996
				PL	B1	176257	31-05-1999
				US	A	5465206	07-11-1995
				US	B1	5465206	21-04-1998
				WO	A1	9512859	11-05-1995
				US	A	6032133	29-02-2000